Cryptographic requirements for chaotic secure communications

Gonzalo Álvarez* and Shujun Li†

Abstract

In recent years, a great amount of secure communications systems based on chaotic synchronization have been published. Most of the proposed schemes fail to explain a number of features of fundamental importance to all cryptosystems, such as implementation details, or key definition, characterization, and generation. As a consequence, the proposed ciphers are difficult to realize in practice with a reasonable degree of security. Likewise, they are seldom accompanied by a security analysis. Thus, it is hard for the reader to have a hint about their security and performance. In this work we provide a set of guidelines that every new cryptosystem would benefit from adhering to. The proposed guidelines address these two main gaps, i.e., correct key management and security analysis, among other topics, to help new cryptosystems be presented in a more rigorous cryptographic way. Also some recommendations are made regarding some practical aspects of communications, such as implementation, channel noise, limited bandwith, and attenuation.

Keywords: Chaos; cryptography; design guidelines

1 Introduction

Modern telecommunications networks, and specially Internet and mobile telephones, have expanded the possibilities of user communications and information transmission to limits unimaginable a short time ago. There is a parallel growing demand of cryptographic techniques, which has originated an intense research activity and the search of new directions in cryptography. As a result, a rich variety of chaotic cryptosystems for end to end communications have been put forward [1, 2], whose robustness and privacy are equally diverse.

There exist two main approaches to chaotic ciphers design: analog and digital. The first one is based on the concept of chaotic synchronization [3]. In these systems, the information can be transmitted by the chaotic signal in a number of ways: chaotic masking [4, 5, 6, 7, 8], in which the analog message signal $m(t)$ is added to the output of the chaotic generator $x(t)$ in the transmitter; chaotic

*Instituto Física Aplicada, CSIC, Serrano 144, 28006, Madrid, Spain, e-mail: gonzalo@iec.csic.es

†Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Toon, HK SAR, China, e-mail: hooklee@mail.com

switching or chaos shift keying (CSK) [9, 10], in which a binary message signal is used to choose between different chaotic attractors; chaotic modulation [11, 12, 13, 14], in which a binary message modulates a parameter of the chaotic generator or when spread spectrum techniques are used to multiply the message signal by the chaotic one; and chaos control [15, 16, 17], in which small perturbations cause the symbolic dynamics of a chaotic system to track a prescribed symbol sequence. Regardless of the method used to transmit the message signal, the receiver has to synchronize with the transmitter's chaotic generator to regenerate the chaotic signal $x(t)$ and thus recover the message $m(t)$.

The second approach to the design of chaos-based cryptosystems consists of using digital computers to iterate a chaotic map and mask the binary message in a number of ways [18, 19, 20, 21, 22, 23]. These ciphers do not depend on synchronization. Instead, they usually use one or more chaotic maps where the initial point x_0 and the parameter value λ play the role of the key.

Most papers on this topic are published in physics and engineering journals and conferences, but not within the cryptography community. This explains why up to date little or no critical analysis has been made about the design process of these cryptosystems nor to the way the results are presented. Quoting Feng Bao [24]: "The common annoying feature of the cryptosystems based on some mathematical models, e.g., those based on chaos systems, is that only the principle is given. They lack details, such as recommended key sizes and key generation steps, etc. Therefore it is not possible for others to implement the ciphers."

We have detected that a systematic approach to the design and security evaluation is missing. To fill this void, in this paper we give some guidelines which should benefit new chaos-based cryptosystems. Following these guidelines, proposed cryptosystems would be presented in a more rigorous cryptographic way. Otherwise, they tend to be information concealment methods to frustrate the casual eavesdropper, but in no case the determined attacker and will not be taken seriously by cryptologists.

The paper is organized as follows. Sec. 2 lists requirements about the minimum practical details of the chaotic implementations that should be provided. In Sec. 3 the most important key related issues are discussed. In Sec. 4 the recommendations about how to make a security analysis are given. In Sec. 5 some basic but decisive considerations about the channel properties are offered. Sec. 6 concludes the paper.

2 The Implementation

For many chaotic systems, only basic concepts are described and implementation details are neglected. However, generally speaking, implementation details are important for cryptanalysts to judge whether or not there exist security defects. Also, it is obvious that the encryption speed and the implementation cost depend on such details. Therefore, the lack of implementation details makes it difficult to estimate the significance of the proposed cryptosystem, i.e. to analyze its security and overall performance.

2.1 The implementation of the chaotic systems

As we introduced in Sec. 1, there are two basic approaches to design chaotic ciphers: analog and digital. The first one is generally based on chaos synchronization, and the concerned chaotic systems are implemented in analog form. The second one is independent of chaos synchronization and the chaotic systems are completely implemented in digital computers. Additionally, in some conditions, the chaotic systems may be implemented in combined form, that is to say, both analog and digital parts are involved.

When analog parts are involved, the circuit diagrams to generate chaos should be given with enough details. When digital parts are involved, the following details should be given: the finite computing precision, the adopted digital arithmetic (fixed-point or floating-point), hardware/software configuration, etc. When both analog and digital parts are involved, details on A/D and D/A interfaces should also be described.

Rule 1 *It should be thoroughly described how to implement the chaotic systems.*

When the chaotic systems are (completely or partially) implemented in digital form, dynamical degradation will occur. This problem has been extensively studied in the last two decades, and it has been clarified that such dynamical degradation may cause security defects in chaos-based cryptosystems. To overcome this problem, some methods should be used to improve dynamical degradation of digital chaotic systems. A considerable countermeasure is to timely perturb the chaotic systems with a small pseudo-random signal. For more details, please refer to §2.5 of [25], in which Shujun Li gives a comprehensive review on this issue.

Rule 2 *For chaotic systems implemented in digital form, the negative dynamical degradation should be taken into consideration.*

2.2 The implementation of the cryptosystem

In the cryptography community, there are two well-known sayings: "it is quite easy to design a secure but very SLOW cipher", and "it is quite easy to design a secure but very LARGE cipher". If the security of a chaotic cryptosystem is reached with the loss of working efficiency, then its significance will be trivial and will not be accepted by pure cryptographers.

Rule 3 *Without loss of security, the cryptosystem should be easy to implement with acceptable cost and should work with acceptable speed.*

3 The key

A fundamental aspect of every cryptosystem is the key. An algorithm is as secure as its key. No matter how strong and well designed the algorithm might be, if the key is poorly chosen or the key space is small enough, the cryptosystem will be broken. Unfortunately, most chaotic secure communications schemes proposed to date fail to clearly, if at all, explain what the key is, how it should be chosen, and to thoroughly describe the available key space.

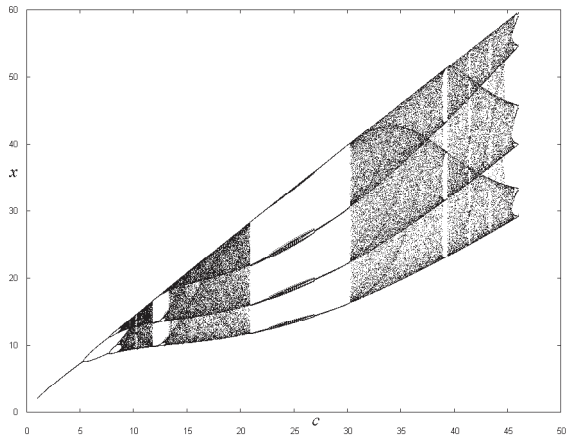

Figure 1: Bifurcation diagram for the Rossler attractor when $a = b = 0.1$ and c is varied.

3.1 Key definition

A cryptosystem cannot exist without a key. Otherwise, it might be considered as a coding system, but never regarded as a secure system. In every cryptosystem an important effort must be devoted to clearly define and characterize the key. Many chaos-based secure communication systems proposed in the literature do not specify what the key is. It is assumed that the key must be made from the parameters of the chaotic system, but it is not clearly stated which parameters are, which their range is and what their precision or sensibility is.

Rule 4 *What the key is should be thoroughly defined.*

3.2 The key space

Once the key has been defined, it is equally important to characterize it, i.e., the key space must be studied in depth.

The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system. The symbol v is used to denote a key and the symbol $\mathbf{V}$ to denote a set of keys. Since the total number of possible keys is equal to $r = |\mathbf{V}|$, the set $\mathbf{V}$ or key space can be expressed as

$$\mathbf{V} = \{v_1, v_2, \ldots, v_r\}. \tag{1}$$

In classical cryptographic algorithms based on number theory, the key is usually a string of random bits generated by some automatic process. If the key is n bits long, then every possible n-bit key must be equally likely, with probability 2^{-n}.

In most chaotic schemes, though, the key space is nonlinear because all the keys are not equally strong. We say that a key is *weak* or *degenerated* if it is easier to break a ciphertext encrypted with this key than breaking a ciphertext encrypted with another key. There exist keys giving rise to non-uniformly distributed chaotic values. As shown in Fig. 1, bifurcation diagrams help to

discover the intervals for which a given parameter originates periodic orbits. These values should be avoided, and the chaotic bands should be preferred.

When many parameters are used simultaneously as part of the key, the mutual interdependence complicates the task of deciding which are the good intervals. In any case, the authors of the proposed cryptosystem should conduct a study of the chaotic regions of the parameter space from which valid keys, i.e., parameter values leading to chaotic behavior, can be chosen. Depending on the number of parameters chosen as part of the key, this region will have $1, 2, 3, \ldots$ dimensions.

A possible way to describe the key space might be in terms of positive Lyapunov exponents. According to [26, p. 196], let $\mathbf{f}$ be a map of $\mathbb{R}^m$, $m \geq 1$, and $\{\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots\}$ be a bounded orbit of $\mathbf{f}$. The orbit is chaotic if

1. it is not asymptotically periodic,
2. no Lyapunov exponent is exactly zero, and
3. the largest Lyapunov exponent is positive.

The largest Lyapunov exponent can be computed for different combinations of the parameters. If it is positive, then the combination can be used as a valid key. In Fig. 3, the chaotic region for the Henon attractor has been plotted following this criterion. This region corresponds to the keyspace. In general, parameters chosen from the lower white region give rise to periodic orbits, while parameters chosen from the upper white region give rise to unbounded orbits. Both regions should be avoided to get suitable keys. Only keys within the black region are good. And even within this region, there exist periodic windows, unsuitable for robust keys.

However, this type of irregular and often fractal chaotic region shared by most secure communication systems proposed is inadequate for cryptographic purposes because there is no easy way to define its boundary. Complete chaoticity for any parameter value should be preferred. A simple map which behaves in this way is the following skew tent map with a control parameter $p \in (0, 1)$ (see also Fig. 2):

$$F(x) = \begin{cases} x/p, & x \in [0, p] \\ (1-x)/(1-p), & x \in (p, 1] \end{cases}. \tag{2}$$

For any control parameter $p \in (0, 1)$, the above piecewise linear map is always chaotic. In fact, for a piecewise linear chaotic map $F : X \to X$, if each linear segment is mapped onto X, the map will be chaotic and have many desired dynamical properties [25, §3.2.1]. Following such a result, as long as the control parameter does not change the mapping of each linear segment onto X, the obtained chaotic map will be good to construct chaotic cryptosystems.

Rule 5 *The chaotic region which constitutes the key space* $\mathbf{V}$ *from which valid keys are to be chosen should be thoroughly specified.*

It is sometimes taken for granted that the security of the encryption scheme is related to the size of the key space. A necessary, but not sufficient, condition for an encryption scheme to be secure is that the key space be large enough

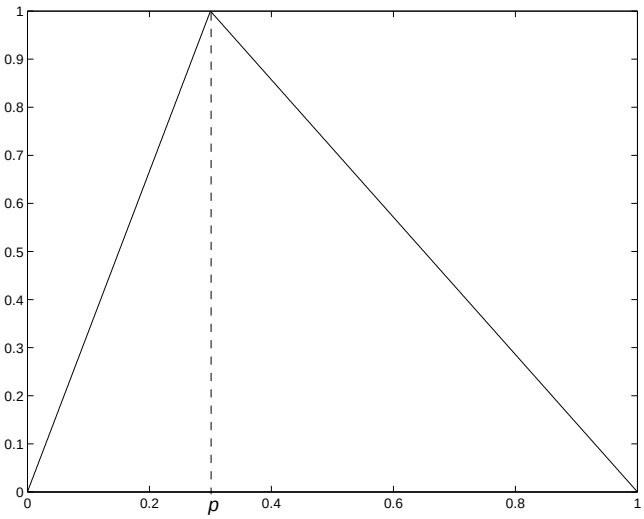

Figure 2: Skew tent map with a control parameter p.

to frustrate brute force attacks (see Sec. 4.4). If the chaotic region does not meet this requirement, then it should be enlarged accordingly. However, the solution is not as simple as discretizing the region with a finer grain, because this could lead to *equivalent* keys, i.e., the same ciphertext is decrypted by two different keys. When two different keys are very close to each other, they could decrypt part or all the ciphertext. The safeguard between adjacent keys should be defined. In other words, the chaotic region should be discretized. In chaotic regime, the sensitivity to parameters will guarantee that two orbits starting from the same initial point but with slightly different parameters will diverge (the divergence rate is given by the Lyapunov exponents). However, the need for synchronization sometimes allows for an important parameter mismatch.

From a cryptographic point of view, the secret parameter should be sensitive enough to guarantee the so-called avalanche property: even when the smallest change occurs for the parameter, the ciphertext will change dramatically. Ideally, mathematical expectation of the change of ciphertext is half of the maximal value of all possible ciphertexts. For example, a natural idea to do so is to iterate the employed chaotic system for multiple times [27].

Rule 6 *The useful chaotic region (the key space* $\mathbf{V}$*) should be discretized in such a way that the avalanche effect is guaranteed: two ciphertexts encrypted by two different keys* v_1, v_2 *chosen as close as possible from the key space* $\mathbf{V}$ *will be entirely different.*

In some chaotic cryptosystems where more than one parameter is used as part of the key, it is possible to fix one of them and try to approximate the others. This is an undesirable behavior. Ideally, when the key is made from a number of parameters, the recovered signal after an illegal decryption attempt should never reveal that the attacker is approaching the exact key when one parameter is slowly varied. In other words, the recovered signal should appear the same if none of the parameters is guessed as if all but one of the parameters

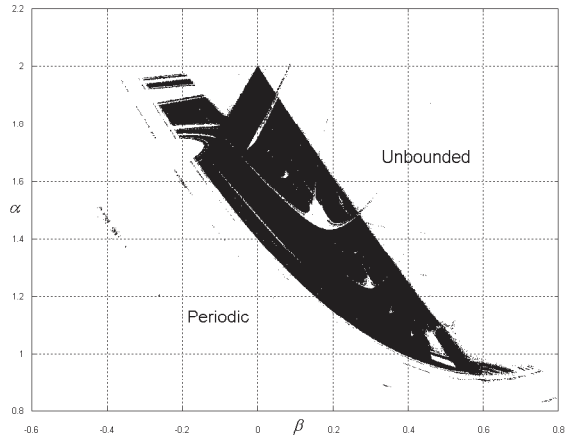

Figure 3: Chaotic region for the Henon attractor.

are guessed. This implies that the total key space is the product, and not the addition, of all the parameters involved.

Rule 7 *Partial knowledge of the key should never imply partial knowledge of the cleartext.*

3.3 Key generation

Once the key has been defined and the key space has been properly characterized, the process to choose good keys should be explained in detail. If some parameter ranges are given and the parameter values can be randomly chosen within these ranges, then it should be clear that there is no possibility of generating weak or degenerated keys.

Sometimes the useful chaotic region has irregular shapes. This shape could be enclosed in a regular one, such as a sphere or a cube, and the key could be chosen randomly within this regular shape and checked whether it is in the useful chaotic region.

Rule 8 *The algorithm or process to generate valid keys from the key space* $\mathbf{V}$ *should be thoroughly specified.*

4 Security analysis

When a new cryptosystem is proposed, it should always be accompanied by some security analysis. Although this analysis cannot comprise all the possible attacks against the newly created cipher, it should include at least the best known attacks and the corresponding results. This analysis helps to spot and correct flaws before the new scheme is published. That a cipher is resilient to all these attacks does not mean that it is secure, but at least it has undergone a certain amount of critical analysis. It is a necessary, but not sufficient, condition for security.

First of all, to resist common attacks, the designed cryptosystem should have the following basic cryptographic properties: confusion and diffusion. The

first property reflects uniformity of all keys, and the second one reflects strong sensitivity (avalanche) of the key to small change. Obviously, Rule 6 mentioned above corresponds to diffusion. Here, we add a rule corresponding to confusion. To achieve confusion, statistical properties of the ciphertext, such as distribution, correlation and differential probabilities, should be independent of the exact value of the key. Many chaos-based cryptosystems are broken because of the lack of confusion property, such as E. Alvarez et al.'s cipher proposed in [22].

Rule 9 *For different keys, no distinguishable difference of the ciphertext should be found from statistical point of view.*

Next we describe the sort of attacks which should be accounted for.

4.1 Classical types of attacks

When cryptanalyzing an encryption algorithm, the general assumption made is that the cryptanalist knows exactly the design and working of the cryptosystem under study, i.e., he knows everything about the cryptosystem except the secret key. This is an evident requirement in today's secure communications networks, usually referred to as Kerchoff's principle [28, p. 24]. According to [28, p. 25], it is possible to differentiate between different levels of attacks on cryptosystems. They are enumerated as follows, ordered from the hardest type of attack to the easiest:

1. Cipher text only: The opponent possesses a string of cipher text, c.
2. Known plain text: The opponent possesses a string of plain text, p, and the corresponding cipher text, c.
3. Chosen plain text: The opponent has obtained temporary access to the encryption machinery. Hence he can choose a plain text string, p, and construct the corresponding cipher text string, c.
4. Chosen cipher text: The opponent has obtained temporary access to the decryption machinery. Hence he can choose a cipher text string, c, and construct the corresponding plain text string, p.

In each of these four attacks, the objective is to determine the key that was used. The last two attacks, which might seem unreasonable at first sight, are very common when the cryptographic algorithm, whose key is fixed by the manufacturer and unknown to the attacker, is embedded in a device which the attacker can freely manipulate. Daily life examples of such devices are electronic purse cards, GSM phone SIM (Subscriber Identity Module) cards, POST (Point Of Sale Terminals) machines, or web application session token encryption.

Many examples of how to break chaotic cryptosystems with known plaintext and chosen plaintext attacks can be found in [29, 30, 31, 32, 33].

Rule 10 *At a minimum, it should be checked whether the cryptosystem is broken by simple known plaintext and chosen plaintext attacks.*

4.2 Chaos-specific attacks

Many different methods have been proposed to attack chaotic encryption schemes, both for analog and digital systems. In this paper we will focus on the former. There are three possibilities for their cryptanalysis [34]:

1. The extraction of the message signal $m(t)$ from the transmitted ciphertext signal $c(t)$.
2. The extraction of the chaotic masking signal $x(t)$.
3. The estimation of the parameters of the chaotic receiver, which are chosen from the key space $\mathbf{V}$.

The extraction of the message signal is generally possible if $m(t)$ is a periodic signal or consists of periodic frames with sufficient duration. It can be accomplished using different methods: spectral analysis techniques [35], autocorrelation and cross-correlation [27], filtering, or time series power estimation.

The chaotic masking signal $x(t)$ can be extracted using time delaying embedding reconstruction or return maps [36, 37, 38, 39].

Parameter identification can be performed using generalized synchronization [40] or spectral analysis. Sometimes it is not even necessary to use approximate parameter values because transmitter and receiver are synchronized even under severe parameter mismatch [27].

Rule 11 *At a minimum, it should be checked whether the cryptosystem is broken by well known chaos-specific attacks.*

Also, as we mentioned above, when chaotic systems are implemented in digital form, the dynamical degradation can also cause security defects, which may bring weak keys and make brute force attacks easier. For examples with security defects caused by dynamical degradation of digital chaotic systems, please see [41, 42] (or Chap. 4 of [25]).

4.3 Application-specific attacks

In some specific applications, there are some special attacks. For example, for digital images (videos), unlike normal one-dimensional data, strong correlation always exists between different pixels (transform coefficients). Such correlation information can be used to develop some correlation-based attacks, if the information is not successfully cancelled in cipher-images/cipher-videos.

In addition, in some applications cryptosystems should be specially optimized to make the encryption more efficient. However, sometimes there exists a tradeoff between efficiency and security, and the increment of efficiency causes decrement of security. For example, encrypting partial data of plain-videos is very useful to promote the encryption speed and make the cryptosystem practical, but it is possible to reconstruct partial visual information of plain-videos from partial non-encrypted data.

It is true that different uses of a same cipher in different applications may cause different levels of security [43].

Rule 12 *At a minimum, it should be checked whether the cryptosystem is broken by well known application-specific attacks. If there exists a tradeoff between efficiency and security, explicit criteria should be given to show how to balance the two factors.*

4.4 Brute force attacks

A brute force attack is the method of breaking a cipher by trying every possible key. The quicker the brute force attack, the weaker the cipher. Feasibility of brute force attacks depends on the key space size r of the cipher and on the amount of computational power available to the attacker. Given today's computer speed, it is generally agreed that a key space of size $r < 2^{100}$ is insecure.

Rule 13 *To prevent brute force attacks, the key space size should be* $r > 2^{100}$.

However, this requirement might be very difficult to meet by some proposed ciphers because the key space does not allow for such a big number of different strong keys. For instance, Fig. 3 was created using a resolution of 10^{-3}, i.e., there are 1400×3000 different points. To get a number of keys $r > 2^{100} \simeq 10^{30}$, the resolution should be 10^{-15}. However, with that resolution, thousands of keys would be equivalent, unless there is a strong sensitivity to parameter mismatch, which is usually lost by synchronization.

5 The channel

Many secure communications systems proposed are tested in Matlab or some other simulation program, but not under real conditions. It should be noted that a real channel is subjected to noise, has a limited bandwith, and is attenuated. When designing a new secure communications scheme, besides security considerations, the channel characteristics should be taken into account, thus preventing the system from failing when tested in a noisy, bandwith-limited, and attenuated channel.

Rule 14 *The secure communications system should work in a channel with* -30 *dB signal/noise ratio, with limited bandwith, and with an attenuation between* -3 *dB and* $+1$ *dB.*

6 Conclusions

We have presented a set of guidelines which are recommended to be adopted by every secure communications systems designer. These guidelines do not constrain the freedom and creativity of the designer, but, if followed, guarantee a reasonable degree of security and cryptographic rigor. In this way, new chaos-based cryptosystems will be easier considered by the cryptography community, and both worlds will be benefited.

Acknowledgements

This research was supported by Ministerio de Ciencia y Tecnología, Proyecto TIC2001-0586.

References

[1] T. Yang. A survey of chaotic secure communication systems. *Int. J. Comp. Cognition*, 2:81–130, 2004.

[2] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Chaotic cryptosystems. In Larry D. Sanson, editor, *33rd Annual 1999 International Carnahan Conference on Security Technology*, pages 332–338. IEEE, 1999.

[3] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64:821–824, 1990.

[4] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. *Int. J. Bifurc. Chaos*, 2:709–713, 1992.

[5] C. W. Wu and L. O. Chua. A simple way to synchronize chaotic systems with applications to secure communications systems. *Int. J. Bifurc. Chaos*, 3:1619–1627, 1993.

[6] Omer Morgul and Moez Feki. A chaotic masking scheme by using synchronized chaotic systems. *Phys. Lett. A*, 251:169–176, 1999.

[7] K. M. Cuomo, A. V. Openheim, and S. H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst – II*, 40:626–633, 1993.

[8] S. M. Shahruz, A. K. Pradeep, and R. Gurumoorthy. Design of a novel cryptosystem based on chaotic oscillators and feedback inversion. *J. Sound and Vibration*, 250:762–771, 2002.

[9] H. Dedieu, M. P. Kennedy, and M. Hasler. Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing. *IEEE Trans. Circuits and Systems – II*, 40:634–641, 1993.

[10] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang. Transmission of digital signals by chaotic synchronization. *Int. J. Bifurc. Chaos*, 2:973–977, 1992.

[11] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua. Spread spectrum communication through modulation of chaos in chuas circuit. *Int. J. Bifurc. Chaos*, 3:469–477, 1993.

[12] K. M. Cuomo and A. V. Openheim. Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.*, 71:65–68, 1993.

[13] M. Feki. An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons and Fractals*, 18:141–148, 2003.

[14] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai. A secure communication scheme based on the phase synchronization of chaotic systems. *Chaos*, 13:508–514, 2003.

[15] S. Hayes, C. Grebogi, and E. Ott. Communicating with chaos. *Phys. Rev. Lett.*, 70:3031–3034, 1993.

[16] S. Hayes, C. Grebogi, E. Ott, and A. Mark. Experimental control of chaos for communication. *Phys. Rev. Lett.*, 73:1781–1784, 1994.

[17] C. Grebogi, Y. Lai, and E. Bolt. Communicating with chaos using two-dimensional symbolic dynamics. *Phys. Lett. A*, 255:75–81, 1999.

[18] M. S. Baptista. Cryptography with chaos. *Phys. Lett. A*, 240:50–54, 1998.

[19] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos*, 8:1259–1284, 1998.

[20] N. K. Pareek, V. Patidar, and K. K. Sud. Discrete chaotic cryptography using external key. *Phys. Lett. A*, 309:75–82, 2003.

[21] W. Wong, L. Lee, and K. Wong. A modified chaotic cryptographic method. *Computer Physics Communications*, 138:234–236, 2001.

[22] E. Álvarez, A. Fernández, P. García, J. Jiménez, and A. Marcano. New approach to chaotic encryption. *Phys. Lett. A*, 263:373–375, 1999.

[23] P. García and J. Jiménez. Communication through chaotic map systems. *Phys. Lett. A*, 298:35–40, 2002.

[24] F. Bao. Cryptanalysis of a new cellular automata cryptosystem. *ACISP*, pages 416–427, 2003.

[25] Shujun Li. *Analyese and New Designs of Digital Chaotic Ciphers*. PhD thesis, School of Electronics & Information Enginnering, Xi'an Jiaotong University, Xi'an, China, June 2003. available online at `http://www.hooklee.com/Thesis/pub.html`.

[26] K. Alligood, T. Sauer, and J. Yorke. *Chaos – An introduction to dynamical systems*. Springer, 1997.

[27] H. Zhou and X. Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits Syst – I*, 44:268–271, 1997.

[28] D. R. Stinson. *Cryptography: theory and practice*. CRC Press, 1995.

[29] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a chaotic encryption system. *Phys. Lett. A*, 276:191–196, 2000.

[30] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Keystream cryptanalysis of a chaotic cryptographic method. *Computer Physics Communications*, 2003.

[31] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a chaotic secure communication system. *Phys. Lett. A*, 306:200–205, 2003.

[32] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of an ergodic chaotic cipher. *Phys. Lett. A*, 311:172–179, 2003.

[33] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a discrete chaotic cryptosystem using external key. *Phys. Lett. A*, 319:334–339, 2003.

[34] T. Beth, D. E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In Yvo G. Desmedt, editor, *Advances in Cryptology - CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 318–331. Springer-Verlag, 1994.

[35] T. Yang, L. B. Yang, and C. M. Yang. Breaking chaotic secure communications using a spectogram. *Phys. Lett. A*, 247:105–111, 1998.

[36] K. M. Short. Unmasking a modulated chaotic communications scheme. *Int. J. Bifurc. Chaos*, 6:367–375, 1996.

[37] K. M. Short. Steps toward unmasking secure communications. *Int. J. Bifurc. Chaos*, 4:959–977, 1994.

[38] G. Pérez and H. A. Cerdeira. Extracting messages masked by chaos. *Phys. Rev. Lett.*, 74:1970–1973, 1995.

[39] T. Yang, L. B. Yang, and C. M. Yang. Cryptanalyzing chaotic secure communications using return maps. *Phys. Lett. A*, 245:495–510, 1998.

[40] T. Yang, L. B. Yang, and C. M. Yang. Breaking chaotic switching using generalized synchronization: Examples. *IEEE Trans. Circuits Syst – I*, 45:1062–1067, 1998.

[41] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Comp. Phys. Comm.*, 153:52–58, 2003.

[42] S. Li, X. Mou, Z. Ji, and J. Zhang. Cryptanalysis of a class of chaotic stream ciphers (in Chinese). *Journal of Electronics & Information Technology*, 25(4):473–478, 2003.

[43] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc., New York, 2000.